

Processo de Auditoria

Relatório de Auditoria ao Sistema de Votação Electrónica – Fase de Simulação

Freguesia de Mangualde

2004-07-12

Conteúdos

1	Introdução	2
1.1	Comissão de auditoria	2
1.2	Fontes de informação	2
1.3	Apresentação do SVE	2
1.3.1	Abertura dos postos de votação e da mesa	3
1.3.2	Votação	4
1.3.3	Fecho dos postos de votação e da mesa e comunicação dos resultados	5
1.4	Resumo da auditoria ao funcionamento do SVE no dia do acto eleitoral	6
1.5	Características do sistema que não foram alvo de observação directa	7
1.5.1	Sistema de configuração pré-eleitoral	7
1.5.2	Mecanismos de registo e comunicação de dados	8
1.5.3	Mecanismos de verificação e recuperação de falhas	8
2	Análise das características do SVE	8
2.1	Segurança (S)	9
2.2	Transparência (T)	9
2.3	Acessibilidade (A)	9
2.4	Características transversais e outros aspectos (O)	9
3	Conclusões e Recomendações	9
3.1	Conclusões	9
3.2	Recomendações	10
4	ANEXO - Grelha para as Conclusões e Recomendações do Relatório de Auditoria ao Sistema de Votação Electrónica (RASVE)	13

1 Introdução

1.1 Comissão de auditoria

A comissão de auditoria CASVE C, constituída por Prof. Doutor João Correia Lopes (relator), Prof. Doutor João Pascoal Faria e Prof. Doutor António Miguel Pontes Pimenta Monteiro, esteve presente nas duas salas (secções 1 e 2) preparadas para a votação electrónica na Escola nº 1 de Mangualde, no dia 13 de Junho de 2004, desde a abertura pelas 7:30 até ao fecho da assembleia de voto pelas 19:30.

1.2 Fontes de informação

Para além de se basear nas observações efectuadas no local da votação electrónica em Mangualde, a análise efectuada baseou-se nos seguintes documentos:

- [1] "Auditoria de Voto Electrónico (Indra)", da Indra, recebido a 16 de Junho de 2004;
- [2] "Máquina de Voto — Manual de Utilizador", da Indra, recebido a 16 de Junho de 2004;
- [3] Mensagem de correio electrónico da Indra, recebida a 1 de Julho de 2004, respondendo às perguntas enviadas por esta comissão de auditoria (CASVE C) no dia 28 de Junho de 2004 por correio electrónico.

Apesar de solicitado, a comissão de auditoria não teve acesso ao equipamento de votação para teste e verificação fora do acto eleitoral, nem teve acesso a mais documentação técnica sobre o sistema pedida na mensagem referida em [3] e nas perguntas preliminares enviadas a 31 de Maio de 2004.

1.3 Apresentação do SVE

O SVE auditado é constituído pelos seguintes elementos:

- Postos de voto: 8 postos de votação fornecidos pela empresa Indra, modelo (Part Number) 0260210000000, 3 dos quais na secção 1 (com números de série 0011, 0069 e 0071) e 5 na secção 2 (com números de série 0022, 0026, 0043, 0065, 0100). Todos os postos de votação estavam equipados com sistema operativo Windows NT, leitor de cartões electrónicos (*smartcards*) e ecrã táctil. Os postos de votação estavam isolados, sendo especialmente desenhados para o efeito. Cada posto de voto continha um ecrã táctil de boas dimensões (15"), protecções que tornavam difícil a sua visualização sem ser pela pessoa que está na sua frente, uma ranhura para a inserção do cartão de votante e uma outra para a saída de relatórios impressos em papel. Um dos postos colocados na secção 1 (com número de série 0069) estava equipado com auscultadores e rato, destinando-se o seu uso aos eleitores com necessidades especiais (invisuais, analfabetos).
- Postos com o caderno eleitoral electrónico: um computador de secretária, com sistema operativo Windows 2000 Server, contendo o caderno eleitoral em formato electrónico em cada secção de voto (ficheiro e aplicação para a respectiva consulta e anotação dos eleitores

que votaram), providenciado pela UMIC e totalmente independente dos postos de votação e *smartcards* providenciados pela Indra, para utilização pelos elementos da mesa eleitoral.

- *Smartcards* para os votantes: conjunto de cartões *smartcard* usados para a votação (em substituição dos boletins de voto). Os cartões disponibilizados encontravam-se já prontos a usar (uma única vez cada cartão) nos postos de votação.
- *Smartcards* para os administradores dos postos de votação: cartões usados pelos elementos da Indra para o arranque e encerramento dos postos de votação.
- *Smartcards* para os elementos da mesa de cada secção (3 *smartcards* para cada secção): disponibilizados pela UMIC, para permitir aos elementos de cada mesa aceder ao caderno eleitoral electrónico.

Para além dos membros da equipa de auditoria e do presidente e de dois escrutinadores da mesa eleitoral (em cada secção), estiveram ainda envolvidos no teste ao voto electrónico um membro do STAPE, 3 técnicos da Indra (para apoio no arranque e encerramento dos postos de votação e aconselhamento aos eleitores sobre a utilização dos postos de votação) e um membro da UMIC que coordenou as operações.

O processo auditado através de observação directa incluiu a abertura dos postos de votação e da mesa; o funcionamento dos postos de votação e da consulta aos cadernos eleitorais para obtenção do *smartcard*; e o fecho e comunicação dos resultados dos postos de votação e fecho da mesa de voto.

1.3.1 Abertura dos postos de votação e da mesa

Pelas 7:40 os elementos da Indra efectuaram a iniciação dos postos de votação. Usando uma chave para abrir a tampa de acesso aos botões da máquina, esta arrancou o Sistema Operativo que, sem requerer qualquer palavra-chave, apresentou a interface com o utilizador da aplicação de voto.

Usando um *smartcard*, o operador (elemento da Indra) pôde ter acesso ao um teclado virtual onde introduziu o código de administração de 8 dígitos (PIN do cartão) que deu acesso ao Menu de Administração. Usou primeiramente a opção de “Impressão de Resultados”, que produziu um relatório em papel, de aproximadamente 5 cm por 12 cm, contendo o estado da máquina (nomeadamente a contagem de votos a zero) e posteriormente, após nova introdução do código de administração, a opção “Abrir Mesa”, que colocou a máquina pronta a aceitar votos.

Este procedimento foi repetido para todas as 5 máquinas da secção 2, onde foi efectuada a observação, tendo os relatórios em papel sido entregues na mesa de voto. Procedimento idêntico foi relatado como tendo acontecido na secção 1.

A iniciação dos postos com os cadernos eleitorais electrónicos foi realizada pela representante da UMIC, que transferiu para cada máquina o ficheiro com o caderno eleitoral da respectiva secção de voto. De seguida, a sessão foi aberta, exigindo a autenticação do presidente da mesa e de 2 escrutinadores, e produzindo automaticamente uma acta de abertura (impressa), com a indicação do número de eleitores inscritos (e a indicação de que nenhum havia ainda votado). A autenticação foi

feita pela leitura de 3 cartões electrónicos (“smartcard”) previamente distribuídos aos 3 membros da mesa autorizados para a abrir e encerrar.

1.3.2 Votação

A votação incluiu a verificação da inscrição dos eleitores nos cadernos eleitorais em formato electrónico e em papel efectuada pelos elementos da mesa e, de forma independente, a escolha e registo do voto realizada em postos de votação isolados.

Podiam estar a exercer o seu direito de voto paralelamente tantos eleitores quantos os postos de votação disponíveis.

1.3.2.1 Verificação da inscrição nos cadernos eleitorais

Cada eleitor que pretendia votar dirigia-se à mesa e apresentava o seu cartão de eleitor e bilhete de identidade. O caderno eleitoral em formato electrónico continha apenas o número e o nome de cada eleitor inscrito para votar na secção de voto, sendo a consulta dos cadernos feita por introdução do número de eleitor, ou na falta deste, pelo nome do eleitor.

Após a verificação da identidade do eleitor e a confirmação de que ainda não havia votado, era-lhe entregue um cartão electrónico (*smartcard* de voto), ainda não utilizado durante o acto eleitoral, que o autorizava a utilizar um dos postos de votação. O cartão era retirado de uma pilha de cartões por usar, não tendo o cartão qualquer relação com o caderno eleitoral electrónico ou com a identidade do votante.

1.3.2.2 Votação propriamente dita

De seguida, o votante dirige-se a um posto de voto livre, em cujo monitor deve encontrar uma mensagem pedindo para introduzir o cartão, e introduz na ranhura própria o smartcard que lhe foi entregue pela mesa.

Aparece-lhe então uma representação do boletim de voto, organizado em duas colunas bem visíveis, com os nomes e símbolos dos concorrentes e um quadrado onde irá aparecer a marca da votação (um X). Todos os elementos de cada concorrente (incluindo o quadrado) estão desenhados dentro de um único rectângulo, existindo ainda uma escolha assinalada como voto em branco.

O eleitor faz a sua escolha tocando em qualquer ponto no interior do rectângulo envolvente dos elementos do concorrente de sua preferência. O quadrado associado é assinalado com um X. É sempre possível alterar a escolha.

Quando considerar que a sua escolha está devidamente assinalada deverá tocar na área desenhada como um botão actuador, no fundo do ecrã, e assinalada com a palavra “Confirmar”.

Aparece então uma caixa de diálogo sobreposta contendo os elementos do concorrente escolhido e perguntando se definitivamente confirma a sua escolha. Para a resposta existem dois botões distintos assinalados com as palavras “Sim” e “Não”. Caso responda “Não” voltará ao ecrã anterior. No caso de responder “Sim”, é apresentado um novo ecrã (inquérito de satisfação) contendo 2 questões, cada uma delas seguida de 2 quadrados, um legendado com “sim” e outro com “não”. Para cada questão o eleitor deveria tocar num dos quadrados, sendo então a sua escolha assinalada

com um X. Finalmente, após as duas questões, terem um X num dos quadrados, o eleitor deveria tocar num outro botão, no fundo deste ecrã, assinalado com a palavra “Final”.

Nesta altura aparece uma mensagem com a indicação de que o processo foi concluído e de que pode ser retirado o cartão. No caso de não ter assinalado uma resposta para as duas questões apareceria uma caixa de diálogo a solicitar a resposta completa. Foi relatado que o cartão é modificado pelo posto de forma a impedir a sua reutilização.

Se o cartão fosse retirado antes de aparecer a indicação de que o poderia fazer, todo o processo seria descartado (não sendo contabilizado o voto e a votação no posto, segundo informação os elementos da Indra), podendo o eleitor repetir todos os passos (neste caso o cartão ainda não teria sido modificado pelo posto).

Durante a fase de votação muitos eleitores foram ajudados pelos elementos da Indra presentes.

1.3.2.3 Confirmação da votação nos cadernos eleitorais

No final da votação, o eleitor dirige-se de novo à mesa, para devolver o cartão e receber de volta os seus documentos de identificação.

Um elemento da mesa assinala no caderno eleitoral de forma definitiva o exercício do direito de voto daquele eleitor.

Outro elemento da mesa guarda o cartão já usado, devolvido pelo eleitor, numa caixa de cartões já usados. Como já foi referido, foi utilizado um cartão diferente para cada eleitor.

Alguns eleitores (em número da ordem de unidades), após receberem o cartão de votação e se dirigirem a um dos postos de votação, declararam desistir da votação. Para esses, o caderno eleitoral não foi assinalado definitivamente como tendo exercido o direito de voto.

1.3.3 Fecho dos postos de votação e da mesa e comunicação dos resultados

No final do acto eleitoral, o caderno eleitoral electrónico foi encerrado e os postos de votação encerrados.

1.3.3.1 Fecho do caderno eleitoral electrónico

O caderno eleitoral electrónico foi encerrado, exigindo para isso, e de forma semelhante à da abertura, a autenticação dos 3 membros da mesa detentores dos cartões previamente distribuídos. Após a confirmação desta autenticação, foi emitida uma acta de encerramento contendo o número de votantes assinalados durante a sessão. Toda a informação foi gravada definitivamente em disco sendo ainda efectuada uma cópia em disquete. A aplicação usada na sessão deixa de poder ser utilizada.

1.3.3.2 Fecho dos postos de votação e comunicação de resultados

A possibilidade de votação em cada um dos postos de votação foi também retirada através da introdução do smartcard do administrador e da senha de administração e da actuação da opção do menu de administração “Fechar Mesa”. Também em cada um dos postos de votação foi ligada uma

linha telefónica analógica à respectiva tomada tendo sido depois transmitidos os resultados para a central da Indra após actuação da opção “Transmissão de Resultados”. Finalmente foi actuada a opção “Impressão de Resultados” que emitiu um relatório em papel que foi entregue à representante da UMIC, seguida da opção “Desligar Máquina” que procede ao fecho dos programas.

A representante da UMIC tinha instruções para não revelar o número de votos obtido por cada candidato (nem mesmo aos elementos da mesa), tendo apenas revelado o número total de votos contados pelos postos de votação em cada sala. Supõe-se que este procedimento será alterado numa situação real.

1.4 Resumo da auditoria ao funcionamento do SVE no dia do acto eleitoral

Durante o tempo em que decorreu a auditoria não foram detectadas falhas de hardware ou de software em qualquer dos equipamentos envolvidos, postos de votação e cadernos eleitorais, nem foram observadas interrupções de funcionamento. Também não foram observadas falhas nos *smartcards*.

Dos 7554 eleitores inscritos, votaram 2353 regularmente (em papel), 1089 eleitores foram assinalados nos cadernos eleitorais como tendo tentado a experiência de voto electrónico (46,3% dos votantes) e 1080 eleitores ficaram registados nos postos de voto como tendo concluído a votação.

As principais dificuldades observadas na utilização dos postos de votação foram as seguintes (ordenadas cronologicamente e não de acordo com a sua importância):

- Alguns votantes tiveram dificuldade em aperceber-se imediatamente por que lado se deviam aproximar do posto de voto. Para tal pode ter contribuído a inexperiência dos eleitores e a ausência de painéis ou barreiras em torno dos postos de votação. Esta dificuldade foi sempre ultrapassada facilmente, com ou sem ajuda dos operadores presentes, e não prejudicou a votação.
- Alguns votantes tiveram dificuldade em encontrar a ranhura para introdução do *smartcard* de forma a iniciar a votação. Para tal pode ter contribuído a inexperiência dos eleitores, a posição demasiado rebaixada dos postos de votação (as pessoas precisavam de se inclinar) e a existência de uma outra ranhura próxima para saída do papel da impressora. Esta dificuldade foi sempre ultrapassada, com a ajuda dos operadores presentes quando necessário, e não prejudicou a votação.
- Alguns votantes não tinham a certeza de ter introduzido bem o cartão. Isto aconteceu com os eleitores que, na primeira tentativa, não introduziram o cartão até ao fim. Note-se que, depois de introduzido o cartão até ao fim, o sistema dá *feedback* apropriado (muda o conteúdo do ecrã). Esta dificuldade foi sempre ultrapassada, com a ajuda dos operadores presentes quando necessário, e não prejudicou a votação.
- Alguns votantes não se aperceberam inicialmente que, após seleccionar a opção de voto pretendida (tocando com o dedo na opção pretendida), era necessário pressionar um botão de confirmar localizado na parte inferior do ecrã. Se retirassem o cartão sem pressionar o botão de confirmar (ou sem realizar os passos subsequentes), obteriam uma mensagem

alertando para o facto do processo não estar concluído. No entanto, essa mensagem podia passar despercebida a votantes menos atentos ou mais apressados. Provavelmente, este problema podia ser minorado se fosse suprimido o botão de confirmar, passando-se imediatamente à janela de diálogo seguinte (ver descrição do processo mais acima na secção 1.2.2.2).

- Os elementos da mesa não realizaram nenhum procedimento sistemático para verificar se o votante concluiu o processo de votação ou não (intencionalmente ou não), e assim minorar o problema referido no ponto anterior. Tecnicamente, bastaria que a mesa analisasse o *smartcard* devolvido pelo votante através de um leitor apropriado (para verificar se já tinha ou não sido usado com sucesso). Será provavelmente por essa razão (em conjunto com as razões apontadas no ponto anterior) que se verificou no final uma discrepância de 9 (em 1089) entre o número de registos (votantes) no caderno eleitoral e o número de registos (votos) nos postos de votação.

Em geral, foi necessária ajuda externa extensa para cerca de 33% dos votantes de forma a concluírem com êxito a votação, tendo o tempo médio de votação sido de 63 segundos (numa pequena amostra observada). Praticamente todos os eleitores interessados concluíram com sucesso a sua votação, tendo apenas uma ou duas pessoas desistido. Em geral, as pessoas pareceram muito satisfeitas com a experiência (esta impressão pode ser confirmada com os resultados dos inquéritos de satisfação promovidos pela UMIC à saída do local de voto).

Foram ainda observadas características do sistema que, na opinião dos auditores, são susceptíveis de causar desconforto ou menor satisfação nos votantes:

- Por baixo dos títulos em português, o sistema mostra subtítulos em inglês (dirigidos a eleitores estrangeiros que votem em Portugal), que poderão causar desconforto nos eleitores que não percebem inglês (esses eleitores vêem um texto que não percebem).
- O questionário de satisfação que, nesta experiência, aparece no ecrã do posto de voto no final do processo de votação electrónica, pode ter prejudicado a percepção com que os eleitores ficaram da simplicidade do sistema.

1.5 Características do sistema que não foram alvo de observação directa

Para além do SVE descrito com base em observações directas efectuadas, e de acordo com os documentos [2] e [3], o sistema de votação electrónica completo inclui ainda um sistema de configuração pré-eleitoral, bem como mecanismos de registo e comunicação de dados, e mecanismos de verificação e recuperação de falhas que não foram alvo de observação directa.

1.5.1 Sistema de configuração pré-eleitoral

De acordo com os documentos [2] e [3], existe um programa para a configuração do processo eleitoral (Pre Electoral), que cria os dados de configuração necessários para o correcto funcionamento da aplicação de votação. Estes dados de configuração são gravados numa Compact Flash (CF) que é lida posteriormente pelo programa de votação no processo de arranque. Segundo [3], os dados de configuração são:

- Identificação da mesa / máquina eleitoral associada à CF.

- Informação de acesso (PIN) para administração, abertura e fecho das urnas.
- Parâmetros gerais de configuração (impressões, acesso a servidor de totalização, ...)
- Configuração eleitoral (eleições e candidaturas) para o círculo eleitoral específico a que está atribuída a máquina de votação em concreto.

Segundo [3], a CF tem ainda estruturas vazias de totalização de resultados em função dos mesmos parâmetros de configuração referidos acima.

1.5.2 Mecanismos de registo e comunicação de dados

Segundo [2] e [3], durante a votação são guardados os votos individuais, os totais de votos por candidatura, o total de votos brancos e o total de votos geral.

Segundo [2] e [3], para cada voto emitido, é guardada a seguinte informação:

- o conteúdo do voto é guardado de forma aleatória (não cronológica) numa base de dados na Compact Flash, bem como num backup da mesma em disco,;
- a hora de emissão do voto é registo num *log* (registo de auditoria), mas sem o conteúdo do voto.

Segundo [2] e [3], é efectuado também um *log* de eventuais intervenções de manutenção realizadas durante o acto eleitoral.

Segundo [2] e [3], após o fecho das urnas, é criado um ficheiro de resultados contendo o total geral de votos, o total de votos brancos e o total de votos por candidatura. Este ficheiro é depois encriptado usando o algoritmo DES. O ficheiro encriptado é enviado para os centros totalizadores, e é copiado para a Compact Flash.

1.5.3 Mecanismos de verificação e recuperação de falhas

Segundo [2] e [3], são efectuadas verificações diversas dos componentes de hardware e software, aquando do arranque e em cada transacção (voto emitido).

Segundo [2] e [3], em caso de falha da aplicação, o sistema pode ser recuperado através do reinício do mesmo, sem perda de transacções.

Segundo [2] e [3], em caso de falha nos dispositivos de armazenamento (disco duro ou CF), é apresentada uma mensagem no ecrã da máquina de voto. O administrador pode então substituir a máquina de voto ou a CF por uma máquina ou CF de *backup*.

2 Análise das características do SVE

Resumem-se de seguida as principais conclusões constantes da grelha de avaliação usada na auditoria efectuada.

2.1 Segurança (S)

Relativamente às características que foi possível verificar na auditoria realizada, não se encontraram falhas.

No entanto, terá de se confirmar se a discrepância observada entre o número total de votos dado pelos postos de votação e o número total de votantes dado pelo caderno eleitoral electrónico se deve a um problema de usabilidade ou erro humano (do votante que abandonou o posto de votação sem concluir o processo de votação, ou da mesa que não manipulou correctamente o caderno eleitoral electrónico), e não a um erro do sistema.

Há também características importantes no capítulo da segurança e fiabilidade que não foi possível verificar nesta auditoria.

A razão para não se atribuir pontuação máxima não tem a ver com falhas de segurança observadas, mas antes com a falta de dados.

2.2 Transparência (T)

A classificação atribuída no capítulo de transparência tem a ver com deficiências encontradas que podem ser facilmente ultrapassadas.

O facto de não ter sido possível nesta auditoria fazer algumas verificações importantes no capítulo da transparência também impede a atribuição de classificação máxima.

2.3 Acessibilidade (A)

Foram encontradas algumas deficiências de usabilidade dos postos de votação, mas que são em geral facilmente ultrapassáveis.

A principal limitação no capítulo da acessibilidade tem a ver com a ausência de suporte para mobilidade, mas essa limitação não tem a ver com os sistemas de votação em confronto, mas antes com o caderno eleitoral electrónico, que funcionou localmente e não em rede.

2.4 Características transversais e outros aspectos (O)

Não há mais características a considerar.

3 Conclusões e Recomendações

Faz-se se seguida um resumo do processo sobre a segurança, a transparência e a acessibilidade.

3.1 Conclusões

Nos aspectos que foi possível observar, pode-se concluir que a experiência de votação electrónica auditada na freguesia de Mangualde decorreu com grande sucesso, sem falhas significativas e com elevada adesão e satisfação dos eleitores. O principal problema observado foi o facto de, para

muitos eleitores, não ter sido evidente quando é que a sua votação electrónica estava concluída, podendo alguns eleitores ter abandonado o posto de voto sem ter concluído a votação, o que poderá explicar a diferença de 9 votos (em 1089) entre o número de registos (votantes) no caderno eleitoral e o número de registos (votos) nos postos de votação.

No entanto, é de salientar que não foi possível efectuar verificações fundamentais no capítulo da segurança, fiabilidade e robustez do sistema, sendo as mais importantes as seguintes (outras verificações não efectuadas são indicadas na grelha em anexo):

- não foi possível verificar a fiabilidade dos postos de votação no que se refere à correcta contabilização do número total de votos em cada opção de voto;
- não foi possível verificar a fiabilidade e segurança das comunicações;
- não foi possível verificar com que facilidade se podem falsificar os *smartcards* usados na votação (trazendo cartões falsos que podem ser usados dissimuladamente para duplicar a votação, ou meios que podem ser usados dissimuladamente para modificar um cartão por forma a permitir a sua utilização repetida);
- não foi possível verificar o bom comportamento dos postos de votação em caso de falha de energia, nomeadamente, se não há perda de votos.

No capítulo da transparência, e segundo [2] e [3], os postos de votação mantêm um registo dos votos individuais, que poderia ser usado para eventual recontagem de votos e, principalmente, como evidência dos votos expressos (de forma equivalente aos boletins de voto em papel depositados nas urnas tradicionais). Mesmo assim, esse registo pode não ser considerado por todos como fornecendo evidência suficiente dos votos expressos, dada a sua natureza "imaterial" e inacessível a pessoas sem conhecimentos informáticos. Uma evidência mais forte seria fornecida por um sistema que imprimisse um boletim de voto em papel com a opção de voto do eleitor. Um sistema desse tipo teria a vantagem adicional de permitir ao próprio eleitor verificar o seu voto de forma definitiva. No entanto, também teria os seus inconvenientes. Segundo [3], o sistema analisado foi desenhado para permitir a impressão de votos, tendo já sido usado com essa configuração em Ushuaia na Argentina, em 2003.

No capítulo da acessibilidade, é de salientar que o sistema auditado não suporta a mobilidade dos eleitores, isto é, não permite que um eleitor vote numa secção de voto diferente daquela que corresponde ao seu número de eleitor. Esta característica teria provavelmente grande acolhimento nos eleitores e poderia contribuir para a redução das taxas de abstenção. Note-se no entanto que a mobilidade dos eleitores não é impedida pelos postos de votação electrónicos (a mobilidade seria possível com ou sem estes postos de votação), mas antes pelo facto dos cadernos eleitorais electrónicos funcionarem localmente e não em rede. De facto, num cenário de mobilidade, seria necessário que os cadernos eleitorais electrónicos estivessem ligados em rede, para impedir que o mesmo eleitor possa votar mais do que uma vez.

3.2 Recomendações

Na auditoria realizado até ao momento, não foi possível verificar um conjunto de aspectos importantes, conforme já foi referido. Assim, recomenda-se que esta auditoria seja alargada com a

recolha e análise da informação em falta (informação a fornecer sobretudo pelo fornecedor do equipamento mas também pela UMIC), bem como com o acesso a equipamentos semelhantes aos usados na experiência de votação electrónica, para efeito de realização de testes em ambiente controlado. Com base nessa informação e nos resultados desses testes, será possível formular conclusões e recomendações mais fundamentadas e com maior alcance.

Em relação às deficiências desde já observadas na auditoria realizada, recomendam-se as seguintes acções correctivas:

- Para ultrapassar ou reduzir os problemas observados no capítulo da usabilidade, recomenda-se:
 - Criar um mecanismo ou procedimento sistemático que permita aos elementos da mesa ter a certeza se um votante conclui ou não a sua votação electrónica com sucesso. Como já foi referido, bastaria que um elemento da mesa passasse o cartão devolvido pelo votante num leitor apropriado.
 - No programa que corre nos postos de votação, considerar a supressão do botão de confirmação, passando-se imediatamente à janela de confirmação da opção de voto seleccionada (conforme explicado acima), com vista a reduzir o número de casos em que as pessoas abandonam o posto de voto sem ter efectivamente concluído o processo de votação. Realizar testes de usabilidade para verificar se tal supressão é efectivamente vantajosa.
 - Considerar um outro mecanismo para suportar a língua inglesa (em vez de subtítulos em inglês por baixo dos títulos em português), e que não seja susceptível de causar confusão aos eleitores que não conhecem essa língua (por exemplo através de bandeiras para mudar de língua, sendo o português a língua que aparece inicialmente a qualquer eleitor).
 - Elevar a posição dos postos de votação, por forma aos eleitores não terem de se inclinar.
 - Rodear cada posto de voto de painéis ou barreiras adequadas, de forma a não deixar qualquer dúvida sobre por que lado os votantes se devem abeirar dos mesmos.
 - Esconder ou tapar a ranhura do papel da impressora, por forma aos votantes não terem qualquer dúvida sobre qual é a ranhura onde devem inserir o cartão.
- Dado que numa situação real não seria adequado ter operadores a ajudar os votantes como aconteceu nesta experiência (pelo menos no mesmo grau), recomenda-se que, numa situação real, esteja disponível em cada local de votação electrónica, antes e durante o período eleitoral, um posto de voto que possa ser usado por um operador para explicar o funcionamento do sistema aos eleitores que o solicitem, e que permita que os próprios eleitores experimentem o sistema sob a supervisão de um operador.
- No capítulo da acessibilidade, para suportar a mobilidade dos eleitores, recomenda-se que seja considerado e analisada a viabilidade de um sistema de caderno eleitoral electrónico em

rede. O principal risco associado a tal sistema tem a ver com a dependência das comunicações. Esse risco poderia ser controlado com o alargamento do período eleitoral em caso de falha de comunicação. Outra dificuldade associada a esse sistema, quando usado em conjunto com o sistema de *smartcards* de voto não reutilizáveis (no mesmo acto eleitoral), tem a ver com a dificuldade de prever o stock de *smartcards* necessário em cada secção de voto, e o previsível aumento do *stock* global necessário. A utilização de *smartcards* deste tipo poderia ter de ser repensada.

- No capítulo da transparência, recomenda-se que seja analisada a pertinência de manter um registo electrónico (ou mesmo um registo em papel, na forma de boletins de voto impressos pelo sistema electrónico) dos votos individuais expressos em cada posto de voto (mantendo o anonimato, de forma semelhante aos boletins de voto em papel depositados nas urnas), de forma a ter uma evidência desses mesmos votos e possibilitar a recontagem dos votos.

4 ANEXO – Grelha para as Conclusões e Recomendações do Relatório de Auditoria ao Sistema de Votação Electrónica (RASVE)

		-							+
SEGURANÇA (S)								X	
<p><i>Relativamente às características que foi possível verificar na auditoria realizada, não se encontraram falhas. No entanto, terá de se confirmar se a discrepância observada entre o número total de votos dado pelos postos de votação e o número total de votantes dado pelo caderno eleitoral electrónico se deve a um problema de usabilidade ou erro humano (do votante que abandonou o posto de votação sem concluir o processo de votação, ou da mesa que não manipulou correctamente o caderno eleitoral electrónico), e não a um erro do sistema. Há também características importantes no capítulo da segurança e fiabilidade que não foi possível verificar nesta auditoria. A razão para não se atribuir pontuação máxima não tem a ver com falhas de segurança observadas, mas antes com a falta de dados.</i></p>									
S	Auditabilidade								
<p>O sistema deverá poder ser auditado quer por observadores externos, quer pelo próprio sistema, com a confrontação dos diversos dados.</p>									
<p><i>Não foi possível verificar.</i></p>									
S	Autenticação do Operador								X
<p>Os utilizadores autorizados a operar o sistema devem ter mecanismos de controlo de acesso não triviais. Os operadores devem ser autenticados pelo sistema através de uma conjugação de alguns dos tipos de autenticação existentes. Por exemplo: cartão inteligente («Smartcard»), PIN ou senha, ou ainda autenticação bio-métrica – impressões digitais, retina ocular e voz.</p>									
<p><i>O administrador dos postos de voto autentica-se com smartcard e password com 8 dígitos, tendo acesso a um menu específico com opções para iniciar e encerrar o processo, imprimir resultados, configurar número de telefone para transmissão de resultados, transmitir resultados e desligar o sistema.</i></p>									
S	Certificabilidade								
<p>O sistema deve poder ser testado e certificado por agentes oficiais.</p>									
<p><i>Não foi possível verificar.</i></p>									
S	Fiabilidade							X	
<p>O SVE deve funcionar de forma fiável, sem perda de votos.</p>									
<p><i>Não foram observadas falhas nos postos de voto, cadernos eleitorais electrónicos ou smartcards, pelos auditores e não foram comunicadas falhas pelos restantes intervenientes (STAP, mesa, UMIC, Indra). No entanto, os auditores não estiveram presentes a 100% do tempo e a acompanhar 100% dos aparelhos (2 salas, 5 + 2 + 1 aparelhos). Verificou-se no final uma inconsistência entre número de votantes indicados no caderno eleitoral electrónico e número total de votos indicados pelas máquinas. Faltou verificar se a comunicação dos resultados para a central é fiável.</i></p>									

S	Isolamento				x	
<p>Só devem existir no SVE os dispositivos de interface externos absolutamente essenciais para o acto eleitoral, sendo todos os componentes certificados e iguais a um padrão, incluindo o software.</p>						
<p><i>Cada máquina de votação encontra-se isolada durante o acto eleitoral, estando apenas conectado o cabo de alimentação (falta verificar se o sistema pode ser comandado pelo cabo de alimentação, como acontece em dispositivos usados em domótica). Excepto na máquina preparada para pessoas com necessidades especiais, alguns dispositivos de interface (tomadas para linha telefónica, rato, auscultadores, e interruptor de alimentação) encontram-se protegidos por uma tampa fechada com chave durante o acto eleitoral, apenas estando acessíveis a ranhura para introdução do cartão de votação e a ranhura para saída de papel da impressora. O sistema não parece ter interfaces de comunicação sem fios (a confirmar). O eleitor tem de inserir um smartcard, mas supõe-se que isso não é susceptível de injeção de código ("vírus eleitoral") no sistema.</i></p>						
S	Segurança das comunicações					
<p>As comunicações entre as assembleias de voto e o sistema central utilizam mecanismos de validação de identidade de ambos (assembleia e sistema central), de não adulteração da informação e de cifragem da mesma para garantir a confidencialidade, integridade e autenticidade.</p>						
<p><i>Não foi possível verificar qual é o protocolo de comunicação usado (para garantir autenticidade e integridade), se há também comunicação de resultados por via tradicional, e não foi efectuada conferência dos resultados recebidos pelas duas vias no receptor. É efectuada comunicação de cada posto de voto para a central da Indra, por modem e linha analógica no final do acto eleitoral, com possibilidade de configurar o número de telefone do destino e visualizar um pequeno "log" do estabelecimento da comunicação. É emitida mensagem de transmissão bem sucedida no final. Da documentação da Indra recebida pode concluir-se que é usada cifragem DES no ficheiro transmitido usando FTP para um servidor RAS.</i></p>						
S	Escalabilidade do Sistema				x	
<p>A arquitectura do sistema possibilita o suporte a um elevado número de eleitores e de assembleias de voto.</p>						
<p><i>1) Tempo que um eleitor demora a votar: Excluindo o questionário final sobre este sistema de votação electrónica (3 toques), são necessários 3 toques para votar (um para seleccionar a opção de voto, outro para pressionar o botão de confirmar no mesmo ecrã, e outro para responder afirmativamente a uma pergunta de confirmação numa janela de diálogo). (O 2º toque poderia ser suprimido tornando o processo mais rápido e igualmente seguro?). É ainda necessário inserir o "smartcard" no início e retirar no final. A resposta do sistema parece rápida. O ideal seria o próprio sistema produzir uma estatística a este respeito. Em resumo, parece ser rápido. 2) Número de máquinas necessárias: não há impedimento técnico a aumentar o número de máquinas, pois funcionam autonomamente. 3) É necessário um smartcard para cada eleitor (pode ser problemático com mobilidade). 4) O caderno eleitoral electrónico funciona localmente num único posto, mas tem um funcionamento simples e rápido. 5) Nesta experiência, as assembleias funcionam autonomamente, e não há impedimento técnico a aumentar o número de assembleias. 6) Ver na comunicação se pode haver congestionamento. 7) Se existisse mobilidade, já poderia ser diferente. 8) Em termos de pessoal de apoio, não parece exigir mais pessoas que um sistema manual, mas pode ser necessário ter pessoas para ajudar os eleitores e postos de teste exteriores à assembleia de voto com ajuda especializada.</i></p>						

TRANSPARÊNCIA (T)						x	
<p><i>A classificação atribuída no capítulo de transparência tem a ver com deficiências encontradas que podem ser facilmente ultrapassadas. O facto de não ter sido possível nesta auditoria fazer algumas verificações importantes no capítulo da transparência também impede a atribuição de classificação máxima.</i></p>							
T	Anonimato					x	
<p>A associação entre o voto e a identidade do eleitor deve ser impossível em qualquer circunstância. A separação destes dados deve garantir a impossibilidade de relacionar o votante com o respectivo voto quer durante a votação (por utilizadores privilegiados, como por exemplo os que realizam manutenção do sistema) quer após a votação (mesmo que por ordem judicial).</p>							
<p><i>Não foi possível observar os logs nas máquinas. É garantido o anonimato porque não há qualquer comunicação entre o caderno eleitoral electrónico ou a identidade do eleitor e o smartcard que é entregue à pessoa para votar na máquina. O "smartcard" é retirado de forma mais ou menos aleatória de uma caixa de smartcards já prontos a usar (na realidade, até podem ser retirados sequencialmente) e, depois de utilizado na máquina de voto, já não pode ser usado 2ª vez, e é colocado numa caixa de cartões já usados. O anonimato poderia ser quebrado no caso da máquina de voto ter um log com a lista de opções de voto seleccionadas por ordem cronológica (ou com o instante de cada voto, ou com o nº do smartcard usado no caso dos smartcards serem usados sequencialmente), e o caderno eleitoral electrónico permitir obter uma lista dos votantes por ordem cronológica (ou com o instante de cada voto). Não foi possível verificar se a opção de voto fica registada no smartcard. Da documentação recebida da Indra podemos concluir que o instante de cada voto (mas não o conteúdo) é guardado num "log", e que o conteúdo de cada voto é guardado numa base de dados (mas sem ordem cronológica).</i></p>							
T	Atomicidade					x	
<p>Garantia de que, em caso de falha a meio do processo, não permanecem registos ou percepções inconsistentes relativos ao mesmo. Por exemplo: registos no caderno eleitoral de votantes, mas sem registos de voto no computador; o eleitor e a mesa ficaram com a percepção de que o voto se concretizou, quando na realidade não ficou nenhum registo no computador; falha de alimentação quando o votante confirma a opção de voto no computador, como se sabe se o voto foi concretizado (por forma a tornar os registos consistentes entre si e consistentes com a percepção das pessoas envolvidas)?</p>							
<p><i>Apesar de não o estar a fazer, a mesa poderia verificar se o eleitor concluiu com sucesso a sua votação, analisando o estado do cartão no final do acto (verificando se está marcado como já usado ou não). Nesta experiência, se a pessoa tirar o cartão sem ter concluído o processo, fica uma mensagem no ecrã que pode ser notada pelas pessoas que estão a acompanhar o processo ou pelo eleitor seguinte. Se a pessoa não chegar a inserir o cartão e não disser nada, só se sabe na contagem final. A mesa só confirma o registo no caderno eleitoral electrónico, depois de a pessoa devolver o smartcard. Se a pessoa desistir a meio do processo, a mesa pode cancelar o registo no caderno eleitoral electrónico, e tem a possibilidade de confirmar que a pessoa de facto não votou verificando se o cartão já está marcado como usado (só quando se conclui o processo é que o cartão fica marcado como usado).</i></p>							

T	Autenticidade (método de autenticação do utilizador)								X
<p>Autenticar o indivíduo é o meio pelo qual a identificação de um votante é validada e confirmada. Apenas os eleitores autorizados devem poder votar. Exemplos de tipos de autenticação são: presencial, PIN, senha, certificado digital, cartão inteligente ou bio-métrica.</p>									
<p><i>O voto é presencial, e o votante tem de apresentar o bilhete de identidade e o cartão de eleitoral, sendo o número de eleitor confrontado com o caderno eleitoral electrónico e de forma redundante no caderno eleitoral em papel.</i></p>									
T	Confiabilidade								X
<p>O SVE deve funcionar de forma fiável e robusta, tornando-se confiável aos olhos dos diversos actores envolvidos, em particular o eleitor.</p>									
<p><i>Sobre Fiabilidade ver acima, sobre a Robustez não foi possível analisar o funcionamento com entradas erradas e condições limite de funcionamento.</i></p>									
T	Documentação técnica								
<p>Todo o projecto e implementação do sistema, inclusive relativamente a testes e segurança do sistema, devem estar documentados, devendo não conter ambiguidades e ser coerente.</p>									
<p><i>Não foi possível verificar.</i></p>									
T	Integridade do Pessoal								
<p>O pessoal envolvido no projecto, implementação, administração e operação do SVE deve ser incorruptível e de integridade inquestionável, inclusive os envolvidos com a distribuição e guarda de dados e equipamentos.</p>									
<p><i>Não foi possível verificar.</i></p>									
T	Integridade do Sistema								
<p>Deve ser possível garantir em qualquer momento que o SVE que está a ser usado é o mesmo que foi validado e certificado por auditores externos, pela Comissão Nacional de Eleições e pelos membros da mesa de voto, eventualmente por um processo de amostragem.</p>									
<p><i>Não foi possível verificar.</i></p>									
T	Não-Coercibilidade								X
<p>O sistema não deve permitir que os eleitores possam provar em quem é que votaram, o que facilitaria a venda ou coerção de votos.</p>									
<p><i>O sistema não imprime nenhum boletim ou comprovativo que possa ser levado pelo votante. Anonimato e votação presencial também ajudam a garantir esta propriedade.</i></p>									
T	Precisão do SVE								
<p>As eleições podem ser decididas por apenas um voto. O sistema não pode tolerar margens estatísticas de erro durante a sua operação.</p>									
<p><i>Tem a ver com outras propriedades: fiabilidade, usabilidade, etc.</i></p>									
T	Privacidade								X
<p>O sistema não deve permitir que alguém tenha o poder de descobrir qual o voto de determinado eleitor, nem que o eleitor possa, mesmo querendo, tornar público o seu voto.</p>									
<p><i>Não foi possível verificar se há logs que permitam saber a ordem de votação e de baixa nos cadernos eleitorais electrónicos. É garantida a privacidade dado o anonimato e por o sistema não imprimir nenhum boletim ou comprovativo que possa ser levado pelo votante.</i></p>									

T	Singularidade (Não Reutilização)					x	
O sistema deve garantir que os eleitores não possam votar mais do que uma vez em cada processo eleitoral.							
<i>O smartcard não pode ser usado 2ª vez, mas é preciso analisar a facilidade com que um votante poderia manipular o cartão de forma a poder ser reutilizado. Depois de votar, o votante fica marcado como tendo votado no caderno eleitoral electrónico e manual. É necessário analisar com que facilidade uma pessoa poderia trazer um smartcard falsificado ou roubado.</i>							
T	Transparência do Processo					x	
Os eleitores devem conhecer e compreender o processo de votação, bem como o funcionamento do SVE se assim o desejarem.							
<i>Existe informação insuficiente na Internet.</i>							
T	Transparência do Sistema						
Todo o software, documentação, equipamento, micro-código e circuitos especiais devem poder ser abertos para inspecção e auditoria a qualquer instante. Deve ser conhecido o formato dos dados registados e transmitidos.							
<i>Não foi possível verificar.</i>							
T	Verificabilidade					x	
O sistema deve permitir verificar que os votos foram correctamente contados, no final da votação, e deve ser possível verificar a autenticidade dos registos dos votos, sem no entanto quebrar outras propriedades como o anonimato ou a privacidade do votante.							
<i>Como não há voto em papel neste sistema, seria preciso ver se ficou algum log no sistema com a lista de opções de voto seleccionadas. Número total de votos expressos pode ser confrontada com número de cartões usados e número de registos no caderno eleitoral. Da documentação recebida da Indra podemos concluir que o sistema permite a impressão em papel do voto expresso, o que já foi usado em 2003 em Ushuaia na Argentina.</i>							
T	Separação de papéis					x	
O fabricante do SVE, o instalador e o operador não devem ser da mesma instituição ou empresa. Os únicos operadores do SVE durante o acto eleitoral devem ser elementos da mesa de voto ou elementos previamente acreditados pela Comissão Nacional de Eleições.							
<i>Os técnicos da empresa Indra abriram e encerraram o processo nos postos de voto.</i>							

ACESSIBILIDADE (A)				x	
Foram encontradas algumas deficiências de usabilidade dos postos de voto, mas que são em geral facilmente ultrapassáveis. A principal limitação no capítulo da acessibilidade tem a ver com a ausência de suporte para mobilidade, mas essa limitação não tem a ver com os sistemas de votação em confronto, mas antes com o caderno eleitoral electrónico, que funcionou localmente e não em rede.					
A	Conveniência				x
O sistema só será útil se permitir aos votantes exercerem o seu direito de voto de forma rápida, com o mínimo de equipamento, treino e sem necessidades específicas adicionais.					
<i>Ver rapidez em escalabilidade. Dificuldades encontradas: perceber por que posição se devem abeirar do sistema (resolve-se com painéis em U), encontrar ranhura para inserir cartão (está muito em baixo e tem ao lado uma ranhura do papel da impressora), perceber se o cartão já está bem introduzido, perceber que não basta seleccionar a opção e é preciso carregar em confirmar. Altear também ajudaria.</i>					
A	Direito de Voto				x
O Direito de Voto será atribuído a um eleitor sempre que ele verifique simultaneamente as propriedades de Autenticidade e Singularidade. Será sempre necessário verificar o Direito de Voto de um eleitor antes de ele poder votar.					
<i>A verificação do direito de voto usa o caderno eleitoral. Ficam dúvidas com respeito à singularidade.</i>					
A	Documentação para eleitor			x	
O eleitor deve ter acesso com a antecedência adequada a informação de compreensão simples sobre o SVE e as suas características.					
<i>Existe um folheto que explica o modo de votar. Possibilidade de teste prévio com ajuda</i>					
A	Flexibilidade				x
Os equipamentos de votação que fazem parte do SVE devem suportar uma variedade de questões relacionadas com o processo de votação, com por exemplo a utilização por pessoas com necessidades especiais, etc.					
<i>Uma das máquinas equipada com rato e auscultadores para pessoas com necessidades especiais (que não sabem ler ou que não vêem). Os botões do rato correspondem a "sim" e "não".</i>					
A	Mobilidade	x			
O SVE pode verificar a propriedade de mobilidade se não houver restrições impostas aos votantes relativamente aos locais de votação.					
<i>Não verifica esta propriedade.</i>					
A	Usabilidade				x
O sistema deve ser de uso fácil e rápido, quer para eleitores quer para operadores (membros da mesa de voto). A interface do SVE, a linguagem e os termos utilizados, deve ser acessíveis aos eleitores e aos elementos que participam no processo eleitoral, não devendo ser necessário que estes tenham conhecimentos informáticos especializados. A localização, orientação e altura do monitor devem ser apropriadas ao eleitor. Um erro involuntário de um eleitor, mal treinado para votar em dado equipamento, pode inverter ou modificar o resultado eleitoral.					
<i>Para eleitores: Devia-se medir objectivamente com base no tempo gasto para concluir e taxa de erros, o que nesta experiência não foi efectuado sistematicamente.</i>					

A	Viabilidade (Custo/Benefício)			x	
O SVE deve ser eficiente e viável economicamente.					
<i>Pode tornar-se dispendioso pois exige um smartcard por votante (ou mais em caso de mobilidade).</i>					